S3-010282

3GPP TSG SA WG3 Security — S3#18

21 - 24 May, 2001

Phoenix, USA

Liaison Statement

From: TSG-SA3

To: ETSI SAGE, GSM Association SG (Security Group)

Cc:

Subject: Reply to LS on the Development of new A5/3

Contact: Charles Brookson
DTI CII3e
Tel: +44 20 7215 3691
Email: cbrookson@iee.org

Attachments: none

3GPP TSG SA3 received a LS from GSMA SG on the Development of the new A5/3 algorithm.

Work plan for information
3GPP TSG SA3 endorses the SAGE work plan for A5/3. SA3 would like to see any further changes and amendments if these are made.

GEA3
SA3 is of the view that there should also be a GEA3 algorithm, based on KASUMI. SA3 would therefore like to see a similar work plan for GEA3 using a 64-bit Key length. SA3 consider the main advantages of GEA3 over GEA2 to be the open publication of the algorithm and that it is a KASUMI-based algorithm. The work on the design of GEA3 is considered of lower priority to the design of A5/3.

A5/3 Kc support for 128 bits
3GPP TSG SA3 considered the change of key to 128 bits. It was thought that the change to 128 bits would be complex and difficult, requiring significant changes to standards throughout GSM.